MacWilliams Extension Theorem for MDS additive codes

Serhii Dyshko

MacWilliams Extension Theorem for MDS additive codes

Serhii Dyshko

IMATH, Université de Toulon, France
dyshko@univ-tln.fr

Abstract. The MacWilliams Extension Theorem states that each linear isometry of a linear code extends to a monomial map. Unlike the linear codes, in general, additive codes do not have the extension property. In this paper, an analogue of the extension theorem for additive codes in the case of additive MDS codes is proved. More precisely, it is shown that for almost all additive MDS codes their additive isometries extend to isometries of the ambient space. There are also described some new classes of additive codes for which an extension theorem holds.

1 Introduction

The MacWilliams Extension Theorem does not have a general analogue neither for nonlinear codes nor for additive codes. Nevertheless, in [1] and [5] the authors observed some classes of nonlinear codes for which an analogue of the extension theorem for nonlinear codes holds. In [3] we proved that the extension theorem for additive codes holds for the codes with the length not greater than some boundary value. There we also proved that, in general, this result cannot be improved.

In this paper, our main objective is to study the extendibility of additive isometries of MDS (maximum distance separable) additive codes. It appears that for almost all MDS codes, except the case of codes of dimension 2, the extension theorem holds, see Proposition 3. In the exceptional case, when code dimension equals 2, we can improve the general result of [3] and increase the bound on the code length, see Proposition 4.

Additionally, we observed an extension theorem for additive isometries of linear codes that are not linear isometries, and an extension theorem for additive isometries of codes of the specified fixed length. The results are formulated in Proposition 5 and Proposition 6 correspondingly.

2 Preliminaries

Let L be a finite field and let m be a positive integer. Consider a Hamming space L^m. The MacWilliams Extension Theorem gives a full description of linear isometries of codes in L^m. It states that each linear isometry of a linear code in L^m extends to a monomial map. A map $f : L^m \to L^m$ is called *monomial* if it

acts by permutation of coordinates and multiplications of coordinates by nonzero scalars. Note that monomial maps describe all isometries of the full Hamming space.

A general analogue of the MacWilliams Extension theorem does not exist for nonlinear codes. There exists an isometry of a nonlinear code that does not extend to an isometry of the whole space (see [1]).

In [3] we observed a generalization of the MacWilliams Extension Theorem for the class of additive codes. A code in L^m is called *additive* if it is an additive subgroup of L^m. An *additive isometry* of an additive code C is an isometry that is a group homomorphism. Evidently, a map f is an additive isometry if and only if f preserves the Hamming weight.

Example 1. Consider an additive code $C = \{(0,0,0),(1,1,0),(\omega,0,1),(\omega^2,1,1)\}$ in $\mathbb{F}_4^3$, where $\mathbb{F}_4 = \{0,1,\omega,\omega^2\}$ and $\omega + 1 = \omega^2$. Define a map $f : C \to L^m$ in the following way: $f\big((0,0,0)\big) = (0,0,0)$, $f\big((1,1,0)\big) = (0,\omega^2,\omega)$, $f\big((\omega,0,1)\big) = (1,0,1)$ and $f\big((\omega^2,1,1)\big) = (1,\omega^2,\omega^2)$. The map f is additive and it preserves the Hamming weight. Therefore f is an additive isometry of the additive code C in $\mathbb{F}_4^3$. Both codes C and $f(C)$ are not $\mathbb{F}_4$-linear.

Let K be a subfield of L. Along with the additive codes we will speak about *K-linear codes*, i.e. codes that are K-linear subspaces of L^m. The notions of additive and K-linear codes in L^m are in some sense equivalent. Any K-linear code is additive and, conversely, any additive code is $\mathbb{F}_p$-linear, where p is the characteristic of L. If $K = L$, a K-linear code is linear. Obviously, any K-linear isometry is additive and any additive isometry is $\mathbb{F}_p$-linear.

Definition 1. *A map $f : L^m \to L^m$ is called* K-monomial *if there exist a permutation $\pi \in S_m$ and automorphisms $g_1,\dots,g_m \in \mathrm{Aut}_K(L)$ such that for all $u \in L^m$,*

$$f(u) = f\big((u_1,u_2,\dots,u_m)\big) = \big(g_1(u_{\pi(1)}), g_2(u_{\pi(2)}),\dots,g_m(u_{\pi(m)})\big)\ .$$

It is an easy exercise to prove that a map $f : L^m \to L^m$ is K-monomial if and only if it is a K-linear isometry.

An extension theorem for K-linear code isometries does not hold in general. For any pair of fields $K \subset L$ there exists a K-linear code and there exists a K-linear isometry of this code that cannot be extended to a K-monomial map. The example observed in [3] follows.

Example 2. Let $m = |K| + 1$. Consider two K-linear codes $C_1 = \langle v_1, v_2\rangle_K$ and $C_2 = \langle u_1, u_2\rangle_K$ of the length $|K| + 1$ with

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & x_1 & x_2 & \dots & x_{|K|} \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 0 & \omega & \omega & \dots & \omega \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}\ ,$$

where $x_i \in K$ are all different and $\omega \in L \setminus K$. Define a K-linear map $f : C_1 \to C_2$ on the generators of C_1 in the following way: $f(v_1) = u_1$ and $f(v_2) = u_2$. The map f is an isometry. But, there is no K-monomial transformation that acts on C_1 in the same way as the map f. The first coordinate of all vectors in C_2 is always zero, but there is no such all-zero coordinate in C_1.

However, we are able to prove an extension theorem for K-linear codes of short length. In [3] we proved the following.

Proposition 1. *Let $K \subset L$ be a pair of finite fields and let $m \leq |K|$. Any K-linear isometry of a K-linear code in L^m extends to a K-monomial map.*

Proof. See [3]. □

According to Example 2, the result of Proposition 1 cannot be improved in general. The aim of this paper is to improve this result for some classes of K-linear codes. Of particular interest are MDS additive codes. The description of the main technique that we use follows.

Denote the degree of the extension $[L : K] = n$. The finite field L is a vector space over K. Fix a K-linear basis $b_1, \ldots, b_n \in L$ of L over K. For a positive integer k and a vector-column $\boldsymbol{v} \in L^k$, let $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n} \in K^k$ be the expansion of $\boldsymbol{v}$ in the basis. This means that $\boldsymbol{v} = \sum_{i=1}^{n} b_i \boldsymbol{v_i}$. Define a *column space* $V \subseteq K^k$ of the vector $\boldsymbol{v}$ as the K-span of vectors, $V = \langle \boldsymbol{v_1}, \ldots, \boldsymbol{v_n} \rangle_K$. Obviously, $\dim_K V \leq n$.

Let C be a K-linear code in L^m and let $f : C \to L^m$ be a K-linear map. Fix a K-linear basis $c_1, \ldots, c_k \in L^m$ of C. Let $A \in \mathrm{M}_{k \times m}(K)$ be a matrix with the rows $c_1, \ldots, c_k$ and let $V_i \subseteq K^k$ denote the column space of the ith column of A, for $i \in \{1, \ldots, m\}$. Call $\mathcal{V} = (V_1, \ldots, V_m)$ a *tuple of spaces* of C. In [3] we proved an important formula for the dimension of a code, $\dim_K C = \dim_K \sum_{i=1}^{m} V_i$.

Let $f : C \to L^m$ be a K-linear map. Let $B \in \mathrm{M}_{n \times k}(K)$ be a matrix with ith row $f(c_i)$, $i \in \{1, \ldots, k\}$. Denote $\mathcal{U} = (U_1, \ldots, U_m)$ the tuple of spaces of $f(C)$, where U_i is the column space of the ith column of B, for $i \in \{1, \ldots, m\}$. Note that the K-linear span of the rows of B equals to the code $f(C)$.

Call $(\mathcal{U}, \mathcal{V})$ a *pair of tuples* that corresponds to the code C and the map f. We say that $\mathcal{V}$ and $\mathcal{U}$ are *equivalent*, and denote $\mathcal{U} \sim \mathcal{V}$, if there exists a permutation $\pi \in S_m$, such that $V_i = U_{\pi(i)}$, for all $i \in \{1, \ldots, m\}$.

Recall for the pair of sets $X \subseteq Y$ the indicator function $\mathbb{1}_X : Y \to \{0, 1\}$ is defined as $\mathbb{1}_X(x) = 1$ for $x \in X$ and $\mathbb{1}_X(x) = 0$ otherwise. In [3] we proved the following.

Proposition 2. *Let $C \subseteq L^m$ be a K-linear code and let $f : C \to L^m$ be a K-linear isometry. Let $(\mathcal{U}, \mathcal{V})$ be a pair of tuples that correspond to C and f. The map f is an isometry if and only if*

$$\sum_{i=1}^{m} \frac{1}{|V_i|} \mathbb{1}_{V_i} = \sum_{i=1}^{m} \frac{1}{|U_i|} \mathbb{1}_{U_i} \,. \tag{1}$$

The map f extends to a K-monomial map if and only if $\mathcal{U} \sim \mathcal{V}$.

Proof. See [3]. □

A solution $(\mathcal{U}, \mathcal{V})$ of eq. (1) is called *trivial* if $\mathcal{U} \sim \mathcal{V}$, and *nontrivial* otherwise. According to Proposition 2, a K-linear code isometry extends to a K-monomial map if and only if the corresponding solution $(\mathcal{U}, \mathcal{V})$ is trivial.

In the case of linear code isometries, when $K = L$, we can easily prove the MacWilliams Extension Theorem using Proposition 2. Indeed, by the construction, in the case $[L : K] = 1$, the spaces that appear in eq. (1) are either lines or zero spaces. Hence, it is easy to see that a solution of eq. (1) can be only trivial.

Let K be a proper subfield of L. Previously, in [3], we proved that for general K-linear codes there exists a nontrivial solution of eq. (1) if and only if $m \geq |K| + 1$. Proposition 1 immediately follows from this fact and Proposition 2.

In the following sections we use the following notation. Let $K \subset L$ be a pair of finite fields, let m be a positive integer and let C be a K-linear code in L^m. Denote $q = |K|$, $k = \dim_K C$ and $n = [L : K]$. Let $\mathcal{V} = (V_1, \ldots, V_m)$ be a tuple of spaces of C. If there is considered a K-linear map $f : C \to L^m$, let $(\mathcal{U}, \mathcal{V})$ be a pair of tuples that correspond to C and f, where $\mathcal{U} = (U_1, \ldots, U_m)$.

3 Extendibility of additive isometries of MDS codes

In coding theory there is a famous Singleton bound according to which the cardinality of a code C in L^m is not greater than $|L|^{m-d+1}$, where d is the minimum distance of the code. The code is called MDS if $|C| = |L|^{m-d+1}$.

In this section we assume that C is a K-linear MDS code of dimension k over K. Since $q^k = |C| = |L|^{m-d+1} = (q^n)^{m-d+1}$, obviously, $k = n(m - d + 1)$. Denote $k_L = m - d + 1$, so that $k = nk_L$. Note that $k_L = \log_{|L|} |C|$ represents an analogue of the dimension of a code in linear case.

Lemma 1. *For each subset $I \subseteq \{1, \ldots, m\}$, $\dim_K \sum_{i \in I} V_i = n \min\{k_L, |I|\}$.*

Proof. It is a well-known fact that a code with minimal distance d is MDS if and only if deleting any $d - 1$ column we get a new code of the same cardinality (see [6]). Let $I \subseteq \{1, \ldots, m\}$ be a set with k_L elements. Let $c_1, \ldots, c_k \in L^m$ be a K-linear basis of C that correspond to the tuple of spaces $\mathcal{V}$ of the code. Consider the K-linear basis $c'_1, \ldots, c'_k$ of a new code C', where each basis vector c'_i is formed from c_i by puncturing the coordinates with indexes $\{1, \ldots, m\} \setminus I$, for $i \in \{1, \ldots, k\}$. The tuple of the spaces $\mathcal{V}' = (V'_1, \ldots, V'_{k_L})$ that corresponds to the basis $c'_1, \ldots, c'_k$ contains only spaces from $\mathcal{V}$ with indexes from I. Hence, using the formula for the dimension of a code, $\dim_K \sum_{i \in I} V_i = \dim_K \sum_{i=1}^{k_L} V'_i = \dim_K C = k$. Moreover, since for all $i \in \{1, \ldots, m\}$, $\dim_K V_i \leq n$ and $k = \dim_K \sum_{i \in I} V_i \leq \sum_{i \in I} \dim_K V_i = |I| n = k$, we have $\dim_K V_i = n$, for all $i \in \{1, \ldots, m\}$.

Now, consider different cases. Evidently, if $|I| \geq k_L$, then $\dim_K \sum_{i \in I} V_i = k$. Let $|I| < k_L$ and let $J \subseteq \{1, \ldots, m\}$ be a subset, such that $I \subset J$ and $|J| = k_L$. Assume that $\dim_K \sum_{i \in I} V_i < n|I|$. Then $\sum_{i \in J} V_i = \sum_{i \in I} V_i + \sum_{i \in J \setminus I} V_i$ and $nk_L = \dim_K \sum_{i \in J} V_i \leq \dim_K \sum_{i \in I} V_i + \dim_K \sum_{i \in J \setminus I} V_i < n|I| + n(|J| - |I|) = n|J| = nk_L$. By contradiction, $\dim_K \sum_{i \in I} V_i \geq n|I|$. Since $\dim_K \sum_{i \in I} V_i \leq n|I|$, we get the statement of the proposition. □

Lemma 1 particularly states that $V_i \cap V_j = \{0\}$ for all $i \neq j$.

Proposition 3. *Let $K \subset L$ be a pair of finite fields. Let C be a K-linear MDS code in L^m with $k_L \neq 2$. Any K-linear isometry of C extends to a K-monomial map.*

Proof. If $k_L = 1$ the statement of the proposition is obvious.

Let $k_L \geq 3$ and therefore $m \geq 3$. Let $f : C \to L^m$ be a K-linear isometry. Assume that f does not extend to a K-monomial map. By Proposition 2, the pair $(\mathcal{U}, \mathcal{V})$ is a nontrivial solution of eq. (1). Using the same idea as in the proof of Proposition 1 (see [3]), we can assume, after a proper reindexing, that there exists a nontrivial covering $V_1 = \bigcup_{i=1}^{t} V_1 \cap U_i$, where $\{0\} \subset V_1 \cap U_i \subset V_1$, for all $i \in \{1, \ldots, t\}$, $t \geq q + 1$. Note that $q = |K| \geq 2$ and therefore $t \geq 3$.

Let $a, b \in K^k$ be such that $a \in V_1 \cap U_1$, $b \in V_1 \cap U_2$ and $a, b \neq 0$. From Lemma 1, $U_1 \cap U_2 = \{0\}$. This implies $a \notin U_2$, $b \notin U_1$, $a + b \notin U_1$ and $a + b \notin U_2$. The element $a + b$ is nonzero since otherwise $a = -b \in U_2$. Also, $a + b \in V_1$ and $a + b \in U_1 + U_2$. In the covering $V_1 \cap U_i$, $i \in \{1, \ldots, t\}$, of V_1 there are at least 3 nonzero spaces, so there exists a space, without loss of generality let it be U_3, such that $a + b \in U_3$. But then $U_3 \cap (U_1 + U_2) \neq \{0\}$, that contradicts to the fact that $\dim_K(U_1 + U_2 + U_3) = n \min\{k_L, 3\} = 3n$. □

For the case $k_L = 2$, the approach presented in Proposition 3 fails. But we still can use the same idea to improve the result of Proposition 1.

Let V be a vector space over K of dimension n. *Partition* of V is a collection of subspaces of V, such that any nonzero vector from V belongs to exactly one subspace from the collection. By $\sigma(n, t)$ we denote the maximum number of subspaces in the partition of V, where t is the maximum dimension of the subspaces in the partition. Let $\sigma(n) = \min_{0 \leq t < n} \sigma(n, t)$. In [7] there are observed different properties of partitions and, particularly, the properties of the value $\sigma(n)$ for different n, and there also is mentioned the general lower bound (with the reference to the result of Beutelspacher [2]), $\sigma(n) \geq q^{\lceil \frac{n}{2} \rceil} + 1$.

Proposition 4. *Let $K \subset L$ be a pair of finite fields. Let C be a K-linear MDS code in L^m with $k_L = 2$ and $m \leq \sqrt{|L|}$. Each K-linear isometry of C extends to a K-monomial map.*

Proof. Assume that $f : C \to L^m$ is an unextendible K-linear isometry. Therefore the pair $(\mathcal{U}, \mathcal{V})$ is a nontrivial solution of eq. (1). As in the proof of Proposition 3, we can assume that the space V_1 is covered nontrivially, $V_1 = \bigcup_{i=1}^{t} V_1 \cap U_i$, where $m \geq t$. Since the code $f(C)$ is also MDS, by Lemma 1, any two different spaces U_i and U_j intersect in zero. Therefore, $V_1 \cap U_i$, for $i \in \{1, \ldots, t\}$, is a partition of V_1 and $m \geq t \geq \sigma(n) > q^{\lceil \frac{n}{2} \rceil} \geq q^{\frac{n}{2}} = \sqrt{|L|}$. By contradiction, the statement of the proposition holds. □

Note that the inequality $m \leq \sqrt{|L|}$ in the proposition is given only for the concreteness. It can be replaced by the inequality $m \leq q^{\lceil \frac{n}{2} \rceil}$ or by a general inequality $m < \sigma(n)$. Although, the exact value of $\sigma(n)$ or more precise bounds on $\sigma(n)$ are known not for many n.

4 Extendibility of additive isometries of linear codes

Whereas the classical MacWilliams Extension theorem describes linear isometries of linear codes in L^m it says nothing about the extendibility of nonlinear isometries of linear codes, particularly, it gives no information about additive isometries of a linear code.

Let C be an L-linear code in L^m. In this section we study the extendibility of K-linear isometries of the code C, considered as a K-linear code.

Denote by k_L the dimension of C over L. Let $A_L \in \mathrm{M}_{k_L \times m}(L)$ be a generator matrix of a linear code C. The rows of the matrix A_L form an L-linear basis of C. Let $b_1, \ldots, b_n$ be a K-linear basis of L over K. Denote by $b_i A_L$ the matrix formed from A_L by multiplying each matrix entry by the scalar b_i, for all $i \in \{1, \ldots, m\}$. Consider a matrix $A = (b_1 A_L^T | \ldots | b_n A_L^T)^T \in \mathrm{M}_{nk_L \times m}(L)$, that is a vertical concatenation of the matrices $b_i A_L$, $i \in \{1, \ldots, m\}$. It is easy to see that the K-linear span of the rows of A gives the code C, and, moreover, the rows of A form a K-linear basis of C. Therefore $k = \dim_K C$ equals to $k_L n$. Denote by $\mathcal{V} = (V_1, \ldots, V_m)$ the tuple of spaces of A.

Lemma 2. *For each $i \in \{1, \ldots, m\}$, $\dim_K V_i = n$ or $\dim_K V_i = 0$. For all $i \neq j$, V_i and V_j either coincide or intersect in zero.*

Proof. Here we prove the first part. The proof of the second part of the statement is more technical and will appear in the full version of the paper. Let $i \in \{1, \ldots, m\}$. The dimension of the space V_i equals to zero if and only if the corresponding ith coordinate in the code is zero. Assume that the ith column of the generator matrix A_L contains a nonzero element $x \in L \setminus \{0\}$. Then the ith column of the generator matrix A contains the elements $b_1 x, \ldots, b_n x \in L \setminus \{0\}$, which form a K-linear basis of L. Hence the column space V_i has dimension $\dim_K V_i \geq n$ and thus $\dim_K V_i = n$. □

Proposition 5. *Let $K \subset L$ be a pair of finite fields. Let C be an L-linear code in L^m with the length $m \leq \sqrt{|L|}$ and let $f : C \to L^m$ be a K-linear isometry such that $f(C)$ is an L-linear code. The map f extends to a K-monomial map.*

Proof. The proof is almost the same as in Proposition 4. Assume that $f : C \to L^m$ is an unextendible K-linear isometry and thus the pair $(\mathcal{U}, \mathcal{V})$ is a nontrivial solution of eq. (1). We can assume that the space V_1 is covered nontrivially, $V_1 = \bigcup_{i=1}^{t} V_1 \cap U_i$, where $m \geq t$. From Lemma 2, since V_1 is nonzero space, $\dim_K V_1 = n$. The code $f(C)$ is also L-linear, and thus from Lemma 2 the spaces $U_1, \ldots, U_m$ or coincide or intersect in zero. Using the same arguments as in the proof of Proposition 4, $m > \sqrt{|L|}$, and therefore, by contradiction, the statement of the proposition is true. □

5 Extendibility of additive isometries of boundary length codes

In this section we consider the case of the K-linear codes of the length $m = q+1$. This is the smallest length of a K-linear code where unextendible K-linear

isometries exist. In our previous works (see [3] and [4]), we made a full description of unextendible K-linear isometries of K-linear codes in L^m, by providing a full description of nontrivial solution of eq. (1), where $m = q + 1$. Based on this full description we formulated one important property of the nontrivial solutions of eq. (1) in the following lemma.

Lemma 3. *Let $(\mathcal{U}, \mathcal{V})$ be a nontrivial solution of eq. (1), where $m = q+1$. There exists a space W of the dimension not greater than $2 + \max_{i\in\{1,\dots,m\}} \dim_K V_i$ such that for all $i \in \{1, \dots, m\}$, $U_i \subseteq W$ and $V_i \subseteq W$.*

Proof. See [4]. □

Using this lemma we make a strong improvement of the general results, presented in Proposition 1, for the K-linear codes of boundary length.

Proposition 6. *Let $K \subset L$ be a pair of finite fields. Let $C \subseteq L^m$ be a K-linear code such that $m = |K| + 1$ and $\dim_K C > [L : K] + 2$. Each K-linear isometry of C extends to a K-monomial map.*

Proof. Assume that $f : C \to L^m$ is an unextendible K-linear isometry. From Proposition 2, the solution $(\mathcal{U}, \mathcal{V})$ of eq. (1) is nontrivial. From Lemma 3, there exists a space W such that for all $i \in \{1, \dots, m\}$, $V_i, U_i \subseteq W$ and $\dim_K W \leq 2 + \max_{i\in\{1,\dots,m\}} \dim_K V_i \leq n + 2$. Obviously, $\sum_{i=1}^m V_i \subseteq W$ and therefore $\dim_K \sum_{i=1}^m V_i \geq \dim_K W$. Using the formula for the dimension of a code, this is equivalent to $\dim_K C = \dim_K \sum_{i=1}^m V_i \leq \dim_K W \leq n + 2$. □

References

1. Avgustinovich, S.V., Solov'eva, F.I.: To the metrical rigidity of binary codes. Probl. Inf. Transm. 39(2), 178–183 (Apr 2003), http://dx.doi.org/10.1023/A:1025148221096
2. Beutelspacher, A.: Blocking sets and partial spreads in finite projective spaces. Geometriae Dedicata 9(4), 425–449 (1980), http://dx.doi.org/10.1007/BF00181559
3. Dyshko, S.: On extendibility of additive code isometries (2014), http://arxiv.org/abs/1406.1714v2
4. Dyshko, S.: Minimal nontrivial solutions of the isometry equation (2015), http://arxiv.org/abs/1501.02470v1
5. Kovalevskaya, D.I.: On metric rigidity for some classes of codes. Probl. Inf. Transm. 47(1), 15–27 (Mar 2011), http://dx.doi.org/10.1134/S0032946011010029
6. MacWilliams, F., Sloane, N.: The Theory of Error-Correcting Codes: Vol.: 1. North-Holland Mathematical Library, North-Holland Publishing Company (1977)
7. Nastase, E.L., Sissokho, P.A.: The minimum size of a finite subspace partition. Linear algebra and its applications 435, 1213–1221 (2011)